OUCH! | 2016. augusztus

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Mi az a zsaroló vírus?**
- **Kifizessük-e a váltságdíjat?**
- **Biztonsági mentés**
- **További védelmi intézkedések**

A zsaroló vírus

Mi az a zsaroló vírus?

A zsaroló vírus, más néven ransomware, a kártékony szoftverek egy különleges fajtája, amely manapság aktívan terjed az interneten azzal fenyegetve áldozatát, hogy elpusztítja az összes dokumentumát és egyéb fájljait. A kártékony szoftverek olyan számítógépes programok, amelyeket a károkozás céljából hoztak létre. A zsaroló vírus egyike ezeknek a kártékony szoftvereknek, és azért örvend népszerűségnek a bűnözők körében, mert elég jövedelmező. Ha a zsarolóvírus megfertőzi a számítógépünket, titkosít bizonyos fájlokat vagy az egész merevlemezt. Kizár minket a rendszerünkből, illetve lehetetlenné teszi a hozzáférést a saját dokumentumainkhoz vagy fotóinkhoz. A zsaroló program ekkor tájékoztat minket, hogy titkosítás feloldásának és a rendszerhez való hozzáférésnek az egyetlen módja váltságdíj fizetése a kiber bűnözőknek (innen a zsaroló vírus megnevezés). A legtöbb esetben a váltságdíjat valamilyen digitális pénzeszközben (pl. Bitcoin) kell kifizetni. A ransomware úgy terjed, mint minden egyéb kártékony szoftver. Ennek leggyakoribb módja a kártékony emailek küldése, amikor a kiber bűnöző rávesz minket arra, hogy egy fertőzött csatolt állományt nyissunk meg vagy egy linkre kattintsunk rá, amely támadó fertőzött weboldalára irányít.

A szerzőről

Lenny Zelster Az NCR vállalat az ügyfeleinek IT üzemeltetését védi, valamint a káros szoftverek elleni küzdelemről tart előadásokat a SANS Intézetnél. A Twitter-en **@lennyzeltser** néven találhatjuk meg, illetve a **zeltser.com**-on vezet blogot.

Kifizessük-e a váltságdíjat?

Ez egy nehéz kérdés. A probléma az, hogy minél gyakrabban fizetünk a bűnözőknek, annál nagyobb lesz a motivációjuk a további fertőzésekre. Viszont előfordulhat, hogy nincs más lehetőségünk az állományaink visszaállítására. Azt azonban tudni kell, hogy még fizetés esetén sincs garancia arra, hogy vissza tudjuk állítani a fájljainkat. Bűnözőkkel állunk szemben, akik egyáltalán nem biztos, hogy feloldják a titkosítást, de ha mégis megkapjuk a feloldás módját a váltságdíjért cserébe, valami bármikor rosszul sülhet el a visszafejtés során, és még az is lehet, hogy a számítógép további kártékony kódokkal van fertőzve.

Biztonsági mentés

A zsarolóvírus fertőzésből váltságdíj fizetése nélkül talán a legjobb visszaállítási módszer a biztonsági mentésből való

A zsaroló vírus

visszaállítás. Ezzel lehetőségünk van a számítógépünk újratelepítése után visszaállítani a fájljainkat akkor is, ha zsarolóvírussal fertőződtünk. Figyeljünk arra, hogy ha a biztonsági mentés a fertőzött gépen található, a zsarolóvírus azt is titkosítja. Ezért fontos, hogy a biztonsági mentéseket egy jó hírű felhőszolgáltatónál helyezzük el, vagy külső tárhelyen tartsuk, ami nincs mindig a rendszerünkhöz csatlakoztatva. További gyakori hiba, hogy az emberek azt hiszik, hogy a biztonsági mentésből való visszaállítás működik tesztelés nélkül is. Győződjünk meg arról, hogy a biztonsági mentéseink működnek és legyünk biztosak abban, hogy vissza tudjuk állítani a fájlokat, ha zsarolóvírus támadná meg a rendszerünket. A biztonsági mentés akkor is jól jön, ha véletlenül törlünk ki fájlokat vagy a merevlemezünk adja meg magát.

A zsaroló vírus egy olyan kártékony program, amely ha egyszer megfertőzi a számítógépünket, az összes rajta lévő állományt titkosítja, megakadályozva a mi hozzáférésünket.

További védelmi intézkedések

Úgy tudunk védekezni a zsarolóvírussal szemben, mint ahogy azt tennénk egyéb kártékony programok ellen: ne fertőződjünk meg. Legyen mindig naprakész a megbízható forrásból beszerzett vírusirtó programunk. Ezeket arra tervezik, hogy megállítsák a kártékony programokat, de ettől még egy vírusirtó nem fog minden kártevőt blokkolni vagy eltávolítani a rendszerünkből. A kiber bűnözők folyamatosan azon dolgoznak, hogy az új és kifinomultabb kártékony programjaik kivédjék az érzékelést. Ezzel szemben, a vírusirtó gyártók új képességekkel fejlesztik a programjaikat, hogy észleljék a kártékony programokat. Ez olyan, mint a fegyverkezés, ahol mindkét fél túl akar tenni a másikon. Sajnos a rosszfiúk mindig egy lépéssel előrébb járnak, ezért szükséges az, hogy biztonsági mentést készítsünk és alkalmazzuk az alábbi lépéseket a további védelem érdekében:

- a kiber bűnözők sokszor sérülékenységek kihasználásával fertőzik meg az eszközeinket. Minél frissebb a szoftverünk, annál kevesebb ismert sérülékenységet tudnak a bűnözők azon kihasználni. Ezért győződjünk meg arról, hogy az operációs rendszerünk, az alkalmazásaink, és az eszközeink automatikus szoftverfrissítésre vannak beállítva.
- a számítógépeken használjunk átlag felhasználói jogosultságot az 'adminisztrátori' vagy 'root' jogosultsággal szemben. Ezzel további védelmet érünk el, mert a legtöbb kártékony program így nem tudja futtatni magát.
- a kiber bűnözők gyakran trükkel érik el, hogy telepítsük a kártékony programokat. Pl. olyan emailt küldenek, ami helyénvalónak tűnik, de tartalmaz egy linket vagy mellékletet. Úgy tűnhet, mintha a levél a bankunktól vagy egy

A zsaroló vírus

ismerőstől érkezett volna, de ha megnyitjuk a melléklete vagy rákattintunk a hivatkozásra, azzal egy kártékony programot aktiválunk a rendszerünkre. Amennyiben egy email sürgető üzenetet tartalmaz, zavaros, esetleg túl jónak tűnik ahhoz, hogy igaz legyen, akkor lehet, hogy egy támadás. Legyünk gyanakvóak! A józan eszünk a legjobb védelmi eszköz.

Úgy védekezhetünk legjobban a zsarolóvírus ellen, ha odafigyelünk, hogy milyen mellékletet nyitunk meg, vagy milyen linkre kattintunk. Legyen továbbá naprakész vírusirtó szoftverünk és készítsünk rendszeresen biztonsági mentést.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Adathalászat:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_hu.pdf
Káros szoftverek:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf
Titkosítás:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_hu.pdf
Biztonsági mentés:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_hu.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Fordította: Birkás Bence

